

REMARKS

1. The claims have been amended to more particularly and distinctly claim the present invention. No new matter has been added. Accordingly, in accordance with this amendment and the following remarks, reconsideration and withdrawal of the rejection of claims 1-18 is respectfully requested. Allowance of this application is respectfully submitted to be proper and is respectfully solicited.

The Rejection of Claims 17-18 Under 35 U.S.C. 101

2. The present invention discloses and claims a method for establishing secured communication, in a computer system or network where, two or more clients communicate via a communication server. The method uses a single communication port such as SSL port 443. The present method provides an improved means for establishing secured communication, where, two or more clients communicate via a communication server using the "Secure Proxy" protocol communication described, that allows true "ubiquitous" access from anywhere-to any location, any platform; to anywhere - any destination, without the need to know the locations or network addresses of the target client. The present invention provides an improved method for establishing secured communication,

where, two or more clients communicate via a communication server using a "Secure Proxy" protocol, preferably using a single communication port, that allows "secure" communication with end-to-end network security from the access client to the target client, and true "ubiquitous" access from anywhere, any platform; to anywhere, any destination. The present method may be used for establishing secured communication, where, two or more clients communicate via a communication server using a "Secure Proxy" protocol, that allows "secure" access with end-to-end network security from the access client to the target client, as well as client security that eliminates security risks of viruses, worms, backdoors, and leaving trails behind access, and true "ubiquitous" access from anywhere, any platform; to anywhere, any destination, any application, and, to provide true "clientless" access that allows remote access without the need to install access software or application software on the access client.

3. Claims 17 and 18 have been amended to more particularly and distinctly claim the present invention. In claims 17 and 18 "Computer software" has been replaced by--**Computer-readable medium encoded with a computer program--**.

4. Claim 17 has also been amended by adding the following:
requesting communication by a client for connection to
a communication server;
receiving said communication request and a handshake
sequence is performed between said client and said
communication server;
establishing a secure connection between said client
and said communication server;
coordinating a new connection with a second client by
the communication server; and
establishing a connection between the two clients via
the communication server wherein said single
communication port allows access from behind network
securing means by establishing a secure proxy
communication between the two clients by utilizing
end-to-end encrypted data transfer that does not
require decryption at said communication server.

Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

5. Claim 18 has been further amended by adding or **any other ports**. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

The Rejection of Claims 1-8 17 and 18 Under 35 U.S.C.

112

6. Claims 1-6 have been amended to more particularly and distinctly claim the present invention. Claims 1-6 have been amended having the following steps included in claim 1 from which claim 2-6 depend:

requesting communication by a client for connection to a communication server;

receiving said communication request and a handshake sequence is performed between said client and said communication server;

establishing a secure connection between said client and said communication server;

coordinating a new connection with a second client by the communication server; and

establishing a connection between the two clients via the communication server wherein said single communication port allows access from behind network securing means by establishing a secure proxy communication between said two clients by utilizing end-to-end encrypted data transfer.

6. Claim 2 has been amended by the addition of or any other port allowing secure communication using SSL or any other protocol.

7. Claim 3 has been amended further by the addition of network securing means such as before firewalls, or network address translation means after firewalls, and using a communication server as a traffic controller.

8. Claim 4 has been further amended by the addition of using said communication server to enable said secure proxy connection to securely transfer end-to-end encrypted communications

9. Claim 5 has been further amended by adding of communications after "management", and supporting multiple application protocols after "said two clients".

10. Claim 6 has been further amended by adding utilizing encrypted end-to-end data transfer that does not have to be decrypted after "said two clients".

11. Claim 7 has been amended by adding requesting communication by a client for connection to a communication server;
receiving said communication request and a handshake sequence is performed between said client and said communication server;
establishing a secure connection between said client and said communication server;
coordinating a new connection with a second client by the communication server; and _____
establishing a connection between the two clients via the communication server wherein said single communication port allows access from behind network securing means by establishing a secure proxy communication between said two clients by utilizing end-to-end encrypted data transfer.

12. Claim 8 has been amended changing "7" to 8, and adding or any other port.

13. It is respectfully submitted that claims 1-8 and 17, and 18 have now been amended to particularly and distinctly claim the present invention. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

**The Rejection of Claims 1,2 5, 7-12, 15, 17 and 18 Under
35 U.S.C. 102 as being anticipated by Jardin et al.**

14. Claims 1,2, 5, 7-12, 15, 17 and 18 were rejected under 35 U.S.C. 102 as being anticipated by Jardin et al., hereinafter Jardin. Reconsideration and withdrawal of this rejection are respectfully requested. The amendment of claims 1-8 and 17, and 18 were discussed above. Claims 1, 2, 5, 7-12, 15, 17 and 18 are currently amended. Claims 9, 10 11, 12, and 15 are currently amended. Claim 10-12, and 15 depend from claim 9. a

15. Claim 9 has been amended adding by changing [[the]] client, to a second client, and adding the following:
wherein said single communication port allows access from behind network securing means by establishing a secure proxy communication between said two clients by utilizing end-to-end secured data transfer.

16. Claim 10 has been amended adding or any other port.

17 Claim 11 has been amended adding utilized.

18. Claim 12 has been amended adding utilized.

19. Claim 15 has been amended changing the dependency to claim 9 and adding using said communication server to enable said secure proxy connection to securely transfer end-to end encrypted communications..

20. The present invention discloses and claims in claim 1, 2,5,7-12,15,17, and 18 a protocol where a secure communication between two or more clients communicating via a communication server may be established. Such communication is secure in a computing device, computer system, or network and Internet communications. Several possible forms of communication sessions may be established. For example, a one-to-one communication session where one client communicates with another client via a communication server. A one-to-many communication session where one client communicates with two or more other clients via a communication server. A many-to-many communication session where two or more clients communicate with two or more other clients via a communication server. The present invention provides end-to-end network security. This end-to-end security allows enhanced network security from client to communication server, communication server to (target) client, and client-to-client communications using a secure network protocol such as SSL. The claimed methodology

provides an improved method for establishing secured communication, where, no direct network access from one client to the other is allowed. All access is managed and controlled by the communication server, and client and resource level access control may be enforced. The method allows for establishing secured communication, where, network and system performance may be enhanced. The clients and communication server may exchange information that does not require data encryption and/or decryption by the communication server. Using the claimed methodology allows for an improved way of establishing secured communication, where clients and communication server may exchange information that can be centrally managed. These include the security policy and access log that are required to provide simplified central security management. The claimed methodology provides an improved means for establishing secured communication, where access transparency, ubiquitous access - from any location, to any destination) may be enhanced. Using "One Port", such as the SSL port 443, access limitations dues to "communication port" restrictions imposed by firewall/proxy, and inconsistent firewall/proxy port configurations may be removed. For example, access from behind the firewall/proxy given the practical but most restricted configurations, to destinations behind the firewall/proxy given the practical but most restricted configurations may also be realized. As claimed in claims 1, 2, 7-12, 15, 17, and 18 such improved methods for

establishing secured communication, where access transparency, ubiquitous access - from any location, to any destination, for client applications may be enhanced. Applications normally not able to traverse firewall/proxy due to port restrictions, using non-secure port(s), using more than one ports; by using the "Secure Proxy" protocol, may no longer be limited to their access, and may able to provide access given the practical but most restricted firewall/proxy configurations. This also allows for greatly enhanced security and network performance. Using a secure communication port, such as the SSL port 443, may reduce network attacks. Secure ports are normally better protected. By comparison, non-secure, popular communication ports, such as the HTTP port 80, FTP port 23, are common targets of hackers and attract a large number of network attacks. Using a secure communication port and especially, a single secure port greatly reduces the chance of being bombarded with network attacks, traffic, and thus the chance of being compromised. As claimed, the present "Secure Proxy" protocol provides one or more protocols which may use one communication port, where, two or more clients communicate securely via a communication server. Using this method security may be enhanced. There is no direct network access from one client to the other. All access is managed and controlled by the communication server, and client and resource level access control may be enforced. It is respectfully submitted that neither Jardin nor any other

references shows, teaches, discloses, or claims such methodology. It is also apparent, as distinct from Jardin, that by using the "Secure Proxy" protocol herein described, security may be enhanced. End-to-end network security from access client to the target client may be enforced. This end-to-end security includes but is not limited to client authentication, and network security such as that provided by a secure network protocol like SSL. This end-to-end security allows enhanced network security for client to communication server, communication server to target client, and client-to-client communications. The "Secure Proxy" protocol claimed herein, network and system performance may be enhanced. The client and communication server may exchange information that does not required decryption by the communication server. As an example, one client encrypts the data, send it to the communication server, without decrypting the data packet, communication server sends the data packet to another client, the destination client decrypts the data packet. The performance of the communication server and the overall communication time is significantly improved comparing the present invention to other solutions that require the additional processing on the communication server., such as To illustrate this limitation seen in Jardin is where one client encrypts the data, sends it to the server, the server decrypts the data packet, examines the content of the packet to decide which target client the packet should be delivered to, encryption the packet. The server then sends the data

packet to another client, the destination client decrypts the data packet. The performance of the communication server and the overall communication time is significantly improved comparing the present invention to other solutions that require the additional processing on the server. As claimed and described, the "Secure Proxy" protocol of the present methodology, security management may be enhanced. The clients and communication server may exchange information that can be centrally managed. These include the security policy and access log that are required to provide simplified central security management. Another benefit of the invention is that using "One Port", access transparency ubiquitous access - from any location, to any destination may be enhanced. Using "One Port", such as the SSL port 443, access limitations due to "communication port" restrictions imposed by firewall/proxy, and inconsistent firewall/proxy port configurations may be removed. For example, access from behind the firewall/proxy given the practical but most restricted configurations, to destinations behind the firewall/proxy given the practical but most restricted configurations may also be realized. Further, in a practical networking environment, the restricted but practical firewall/proxy configuration is: No inbound connection allowed, and only allows outbound connection to the HTTP port 80 and the SSL port 443 through proxy server. A transparent communication method has to work within such constraints. Using the present method, access transparency, ubiquitous

access - from any location, to any destination, for client applications may be enhanced. Applications normally not able to traverse firewall/proxy due to port restrictions, using non-secure port(s), using more than one ports; by using the "Secure Proxy" protocol, may no longer be limited to their access, and may able to provide access given the practical but most restricted firewall/proxy configurations.

21. It was stated in the Office Action that Jardin anticipates the method in claim 1 which is currently amended. Reconsideration and withdrawal of this rejection is respectfully requested. First it is noted that although Jardin does disclose the use of a single port, and discloses and claims a method for managing secure client-server transactions. Jardin does not, however, disclose teach, claim or suggest in any manner the present invention as claimed in claim 1 where a communication server (proxy server) connects clients via a single port, where a new connection via the communication server (proxy server) is established, where end-to-end secured data is transmitted which does not need to be decrypted at the communication server, and provides all of the advantages described above, as well as the ability to support many application protocols. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

22. It was further argued that Freed et al, hereinafter, Freed establishes that SSL communication occurs on port 443. This is correct, however, neither Jardin or Freed, either alone or in combination disclose, teach claim or suggest the use a single port where a communication server (proxy server) transmits end-to-end, secured data which does not have to be decrypted at the communication server, allowing for one port to support single or multiple application protocols, and enabling all of the advantages described above. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

23. Regarding claims 2, 8, 10 and 18. Claim 2 depends from independent claim 1, claim 8 depends from independent claim 9, and claim 18 depends from independent claim 17, all currently amended, incorporate all of the subject matter of claims 1, 7, 9, and 17 respectively and add additional subject matter thereto, making them a fortiori and independently patentable over the cited reference. It is noted that independent claims 1, 7, 9, and 11 all claim a communication server (proxy server) connecting clients via a single port, where a new connection via the communication server (proxy server) is established, where end-to-end secured data is transmitted which does not need to be decrypted at the communication server, allowing the ability to support many application protocols at the same time. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

24. Regarding the rejection of claims 5 and 15 it is noted that claim 5 depends from independent claim 1, and claim 15 depends from independent claim 9. Both independent claims 1 and 9 are currently amended as noted above. Accordingly, claims 5 and 15 incorporate all of the subject matter of claims 1, 9, respectively and add additional subject matter thereto, making them a fortiori and independently patentable over the cited reference. It is noted that independent claims 1, and 9, both claim a communication server (proxy server) connecting clients via a single port, where a new connection via the communication server (proxy server) is established, where end-to-end secured data is transmitted which does not need to be decrypted at the communication server, allowing the ability to support many application protocols at the same time. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

25. Regarding the rejection of claim 7 currently amended, it was argued that Jardin discloses a "communication proxy server (column 8, lines 2-17). It is respectfully submitted that Jardin does not disclose a communication proxy server at this section nor at any other section of his disclosure. Further in this section Jardin actually teaches away from the present invention in that he uses a server which must decrypt data packages from a client and then re-encrypt prior to sending them to a broker. This is vastly different from the present invention as disclosed

and claimed, as data transfers do not have to be decrypted at the communication server and in fact at encrypted end-to-end as seen in Fig. 1. Further, neither Jardin nor Freed, either alone or in combination disclose teach, claim or suggest in any manner the present invention as claimed in claim 1 where a communication server (proxy server) connects clients via a single port, where a new connection via the communication server (proxy server) is established, where end-to-end secured data is transmitted which does not need to be decrypted at the communication server, and may support many application protocols at the same time. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

26. Regarding claim 9 currently amended, it was argued that Jardin teaches a method for secure communication where "requesting a communication by a client for connection to a "communication server (i.e. broker). It is respectfully submitted that the broker in Jardin disclosure in no way is equivalent to the communication server (proxy server) or the present invention. In fact, in Jardin the broker operates within the disclosed methodology, not a communication server device as described in the present invention which operates as a proxy server. Further, none of Jardin's method for establishing secure communications discloses or teaches the methodology of claim 9. where a communication server (proxy server) connects clients via a single port, where a new connection via the communication server (proxy server) is established, where end-to-end secured data is

transmitted which does not need to be decrypted at the communication server, and which may support many application protocols at the same time. Jardin does disclose the use of a single secure communication port, and Freed does show that SSL communication occurs on port 443, but neither, either alone or in combination disclose, teach, claim, or suggest in any manner the above novel protocol of the present invention. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

27. As for claim 11, which is currently amended, it is noted that claim 11 depends from independent claim 9. Accordingly, claim 11 incorporates all of the subject matter of claims 9, and adds additional subject matter thereto, making it a fortiori and independently patentable over the Jardin. Claim 11 further adds the use of a secure port, which with the limitations of independent claim 9, claims a communication server (proxy server) connecting clients via a single port, where a new connection via the communication server (proxy server) is established, where end-to-end secured data is transmitted which does not need to be decrypted at the communication server, allowing the ability to support many application protocols at the same time. Accordingly, reconsideration and withdrawal of this rejection is respectfully.

28. As for claim 12, which is currently amended, it is noted that claim 12 depends from independent claim 9. Accordingly, claim 12

incorporates all of the subject matter of claims 9, and adds additional subject matter thereto, making it a fortiori and independently patentable over the Jardin. Claim 12 further adds the use of multiple protocols, which with the limitations of independent claim 9, claims a communication server (proxy server) connecting clients via a single port, where a new connection via the communication server (proxy server) is established, where end-to-end secured data is transmitted which does not need to be decrypted at the communication server, allowing the ability to multiple application protocols at the same time. Accordingly, reconsideration and withdrawal of this rejection is respectfully.

29. Regarding claim 17, which is currently amended, claims a computer-readable medium encoded with a computer program for secure communication in a computer system, including means for using a single secure communication port for secured communication within the computer system for establishing secured communications between two or more clients; requesting communication by a client for connection to a communication server; receiving the communication request and a handshake sequence is performed between said client and the communication server; establishing a secure connection between the client and the communication server; coordinating a new connection with the clients by the communication server; and establishing a connection between the two clients via the communication server wherein the single communication port allows access from behind

network securing means by establishing a secure proxy communication between the two clients by utilizing end-to-end secured data transfer that does not require decryption at the communication server. Although Jardin does disclose the use of a single communication port, and Freed discloses SSL communication occurs on port 443, neither reference either alone or in combination discloses, teaches, claims or suggest in any manner the other critical steps in the present invention as claimed in claim 17, namely, the connection via a communication server (proxy server), the coordination of new communication connections using the communications server (proxy server), the end-to end secured (encrypted) data transfer which does not have to be decrypted at the communication server (proxy server), and the novel results obtained therefrom as previously described. Accordingly, reconsideration and withdrawal of this rejection is respectfully.

The Rejection of Claims 3, 4, 6, 13, 14, and 16 Under 35 U.S.C. 103 on Jardin IVO McCurley

30. Claims 3, 4, 6, 13, 14, and 16 were rejected under 35 U.S.C. 103 as unpatentable over Jardin in view of McCurley et al., hereinafter McCurley. As discussed above Jardin discloses a method for managing secure client-server transactions but does not disclose, teach, claim, or suggest the use of a proxy server utilizing end-to-end encrypted data transfer which does not have to be decrypted at the server, that uses one port which can

support many application protocols as disclosed in the present invention and claimed in independent claims 1 and 9. McCurley discloses a method for networking multiplexing and tunneling in single Transmission Control Protocol in a network. McCurley does not disclose, teach, claim, or suggest the use of a proxy server utilizing end-to-end encrypted data transfer which does not have to be decrypted at the server, that uses one port which can support many application protocols. As neither Jardin nor McCurley either alone or in combination disclose, teach, claim or suggest the novel methodology of claim 1 and 9, and since such novel methodology produce new and unexpected results, namely, a secure method for secured communication which has end-to-end security, where no direct network access from one client to another is allowed and the communication is controlled by the communication server. The client and communication server may exchange data which does not require data encryption and/or decryption by the communication server. Further this allows for ease of simplified management of information such as security policy and access logs. Further, the present method as claimed in both claim 1 and 9, provides an improved means for establishing secured communication, where access transparency, ubiquitous access, from any location to any destination is permitted.

31. Claim 3 depends from independent claim 1, and claim 13 depends from independent claim 9. Claims 3 and 13 therefore incorporate all of the subject matter of claim 1, and 9,

respectively, and add additional subject matter thereto to the limitations in their respective base independent claim, thereby making them. a fortiori and independently patentable over the cited reference. Claims 3 and 13 claim access from behind network securing means such as firewalls or network address translation means, by using a single secure communication port by establishing a secure proxy connection between two clients. In addition, claim 3 and 13 use a communication server (proxy server) as a traffic controller. Accordingly, reconsideration and withdrawal of this rejection is respectfully.

32. Regarding claim 4 and 14, as discussed above, Jardin discloses a method for managing secure client-server transactions but does not disclose, teach, claim, or suggest the use of a proxy server utilizing end-to-end encrypted data transfer which does not have to be decrypted at the server, that uses one port which can support many application protocols as disclosed in the present invention and claimed in independent claims 1 and 9. McCurley discloses a method for networking multiplexing and tunneling in single Transmission Control Protocol in a network. McCurley does not disclose, teach, claim, or suggest the use of a proxy server utilizing end-to-end encrypted data transfer which does not have to be decrypted at the server, that uses one port which can support many application protocols. As neither Jardin nor McCurley either alone or in combination disclose, teach, claim or suggest the novel methodology of claim 1 and 9, and

since such novel methodology produce new and unexpected results, namely, a secure method for secured communication which has end-to-end security, where no direct network access from one client to another is allowed and the communication is controlled by the communication server. The client and communication server may exchange data which does not require data encryption and/or decryption by the communication server. Further this allows for ease of simplified management of information such as security policy and access logs. Further, the present method as claimed in both claim 1 and 9, provides an improved means for establishing secured communication, where access transparency, ubiquitous access, from any location to any destination is permitted. Claim 4 depends from independent claim 1, and claim 14 depends from independent claim 9. Claims 4 and 14 therefore incorporates all of the subject matter of claim 1, and 9, respectively, and add additional subject matter thereto to the limitations in their respective base independent claim, thereby making them. a fortiori and independently patentable over the cited reference. Claims 4 and 14 claim access from behind firewalls by using a single secure communication port by establishing a secure proxy connection between two clients. In addition, claim 4 and 14 use a communication server (proxy server) to enable a secure proxy connection to securely transfer end-to-end secured communications. Accordingly, reconsideration and withdrawal of this rejection is respectfully.

33. Regarding claims 6 and 16 currently amended, claim 6 depends from independent claim 1, and claim 16 depends from independent claim 9. Claims 6 and 16 therefore incorporate all of the subject matter of claim 1, and 9, respectively, and add additional subject matter thereto making them a fortiori and independently patentable over the cited reference. The discussion above of the limitations in independent claims 1 and 9 is included herein by reference. Claims 6 and 16 claim access from behind firewalls by using a single secure communication port by establishing a secure proxy connection between two clients. In addition, claim 6 and 16 further utilize end-to-end secured data transfer that does not have to be decrypted at the communication server. Accordingly, reconsideration and withdrawal of this rejection is respectfully.

34. The cited but not relied upon references have been carefully reviewed and it is respectfully submitted that none, either alone or in combination with any other reference, disclose, teach, claim or suggest the present invention as claimed.

Conclusion

35. For all of the reasons given above, this application is now respectfully submitted to contain claims which define a

novel, patentable, and truly valuable invention. Hence allowance of this application is respectfully submitted to be proper and fair, and is respectfully solicited.

Very respectfully,



Jeffrey Hall, Attorney for Applicant
Reg. No. 32570
212 Clinton Street
Santa Cruz, CA. 95062
(831) 423-1365

Certificate of Mailing

I hereby certify that this correspondence will be placed in an envelope marked "First Class Mail", addressed to Commissioner for Patents, PO Box 1450, Alexandria, VA. 22313-1450, and affixed with adequate first class postage, and that such envelope will then be sealed and deposited in an approved United States Postal Service deposit box on the date below.

Date: July 2, 2007



Jeffrey Hall

Reg. No. 32570
212 Clinton Street
Santa Cruz, CA. 95062
Tel: (831) 423-1365